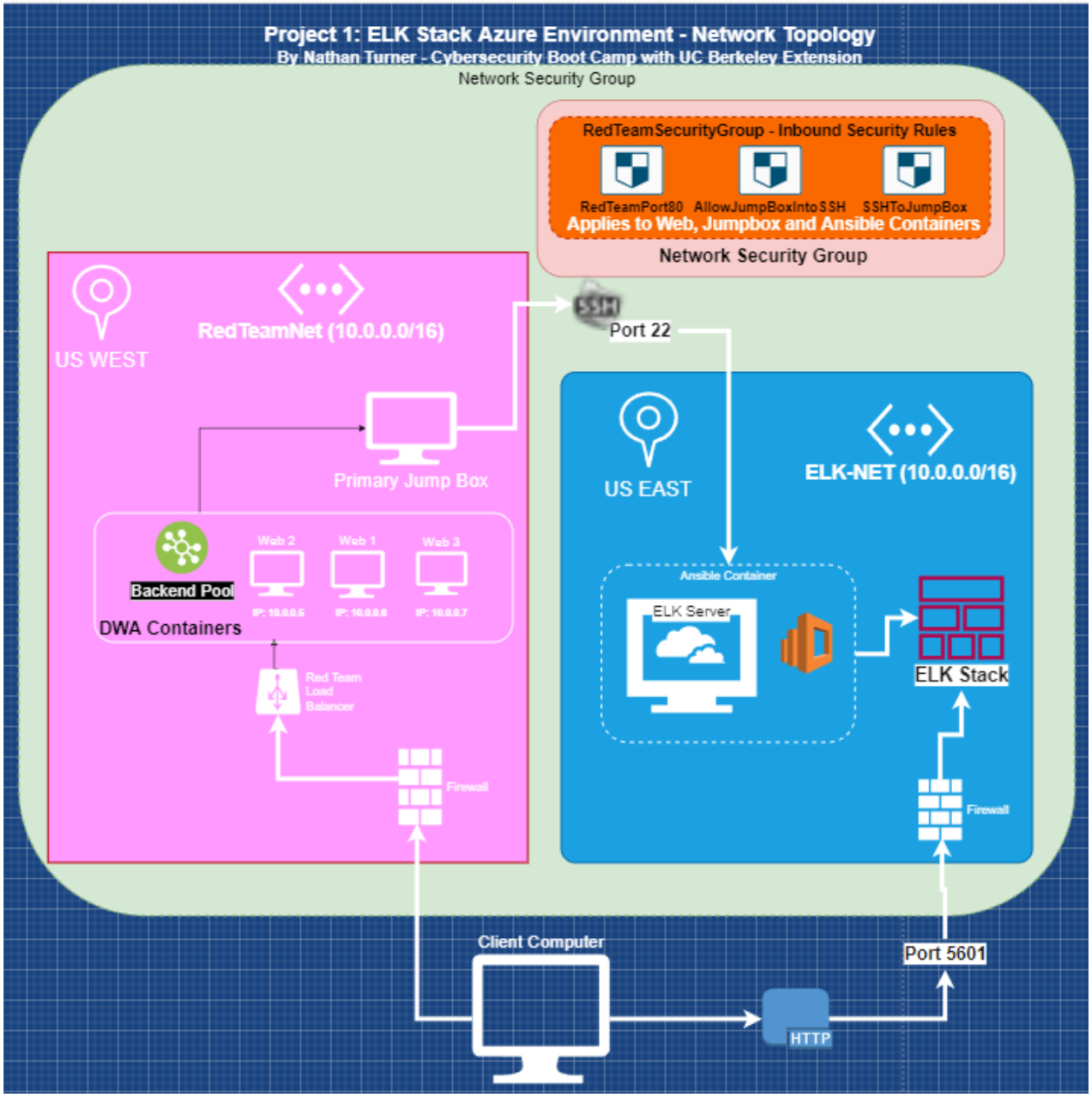
Project 1: Automated ELK Stack Deployment:

The files in this repository were used to configure the network depicted below.



These files have been tested and used to generate a live ELK deployment on Azure. They can be used to either recreate the entire deployment pictured above. Alternatively, select portions of the _____ file may be used to install only certain pieces of it, such as Filebeat.

- Install-elk.yml: Modifies virtual memory and enables configuration of Docker VMs in Ansible for DVWA Container.
- Filebeat-config.yml: The configuration file for
- Filebeat-playbook.yml: The playbook that allows installation of Filebeat to the ELK Stack.
- Metricbeat-config.yml: The configuration file for
- Metricbeat-playbook.yml: The playbook that allows installation of Metricbeat to the ELK Stack.

This document contains the following details:

- Description of the Topology
- Access Policies
- ELK Configuration
    - Beats in Use
    - Machines Being Monitored
- How to Use the Ansible Build

Description of the Topology

The main purpose of this network is to expose a load-balanced and monitored instance of DVWA, the D*mn Vulnerable Web Application.

Load balancing ensures that the application will have high availability, in addition to restricting access to the network.

- Load balancers protect against Distributed Denial of Service Attacks (DDoS), shifting hostile incoming network packets elsewhere, as well as monitoring systems for potential request overload.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the _____ and system _____.

- Filebeat watches for, centralizes, and forwards log data for analysis and indexing.
- Metricbeat collects operating system metrics for analysis & exporting to neighboring services for visualization.

The configuration details of each machine may be found below. Note: Use the Markdown Table Generator to add/remove values from the table.

Name	Function	IP Address	Operating System
ELK-Server	Facilitation of Elasticsearch, Logicstash, Kibana	10.1.0.4	Ubuntu 18.04 (Linux)
Jumpbox	Gateway	10.0.0.1	Ubuntu 18.04 (Linux)
Web-1	Container for DVWA	10.0.0.5	Ubuntu 18.04 (Linux)
Web-2	Container for DVWA	10.0.0.6	Ubuntu 18.04 (Linux)
Web-3	Container for DVWA	10.0.0.7	Ubuntu 18.04 (Linux)

Access Policies

The machines on the internal network are not exposed to the public Internet.

Only the Jumpbox machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

- 50.18.75.167.

Machines within the network can only be accessed by connecting to the jumpbox with a valid SSH key with a whitelisted private IP address..

- The Jumpbox was the machine that was configured & allowed to access the ELK VM?
- The Jumpbox's public IP address is 40.78.52.137, and its private IP address is 10.0.0.4.

A summary of the access policies in place can be found in the table below.

Name	Publicly Accessible	Allowed IP Addresses
ELK-Server	No	10.0.0.4
Jump Box	No	50.18.75.167.
Web-1	No	10.0.0.4
Web-2	No	10.0.0.4

Web-3	No	10.0.0.4

Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because:

- The automated scripts built increase scalability, meaning it can be used on any number of machines to deploy additional ELK stacks as needed or as an organization grows.

The playbook implements the following tasks:

- In 3-5 bullets, explain the steps of the ELK installation play. E.g., install Docker; download image; etc.
- We begin by creating a virtual network, with machines in a different region than our Web/Jumpbox network of machines. A peering is then created to connect them, and the same resource group must be used on the original virtual machine.
- Afterwards, a new VM is created, and the IP address of this VM is added to the Jumpbox's ansible host files.
- Finally, a playbook for Docker.io & python3-pip installation is created & tested in the container.

The following screenshot displays the result of running `docker ps` after successfully configuring the ELK instance.

- Update the path with the name of your screenshot of docker ps output

Target Machines & Beats

This ELK server is configured to monitor the following machines:

- List the IP addresses of the machines you are monitoring. We are monitoring Web-1 (10.0.0.5), Web-2 (10.0.0.6), and Web-3 (10.0.0.7).

We have installed the following Beats on these machines:

- Filebeat & Metricbeat are successfully installed.

These Beats allow us to collect the following information from each machine:

- In 1-2 sentences, explain what kind of data each beat collects, and provide 1 example of what you expect to see. E.g., `Winlogbeat` collects Windows logs, which we use to track user logon events, etc.
- Metricbreat collects & logs systems files for system level analysis.
- Filebeat monitors location files.

Using the Playbook

In order to use the playbook, you will need to have an Ansible control node already configured. Assuming you have such a control node provisioned: SSH into the control node and follow the steps below:

- Copy the file to Ansible configuration file to /etc/ansible to begin the process of running the created playbook(s).
- Update the Ansible host file to include the internal addresses of all web & ELK stack servers.
- Run the playbook, and navigate to the Kibana web page to check that the installation worked as expected.

Answer the following questions to fill in the blanks:

- Which file is the playbook? Where do you copy it? "Install-elk.yml" is the playbook file, which was copied to the /ansible directory.
- Which file do you update to make Ansible run the playbook on a specific machine? How do I specify which machine to install the ELK server on versus which to install Filebeat on? You must update the filebeat-config.yml file, specifying the host IP address for Kibana.
- Which URL do you navigate to in order to check that the ELK server is running? http://[ELKSERVER_ip address]:5601/app/kibana/home

As a Bonus, provide the specific commands the user will need to run to download the playbook, update the files, etc.

-ssh redadmin@jump-box-ip-address

-sudo docker pull [name of container]

-sudo docker run [name of container] bash

-sudo docker start [name of container]

-sudo docker attach [name of container]

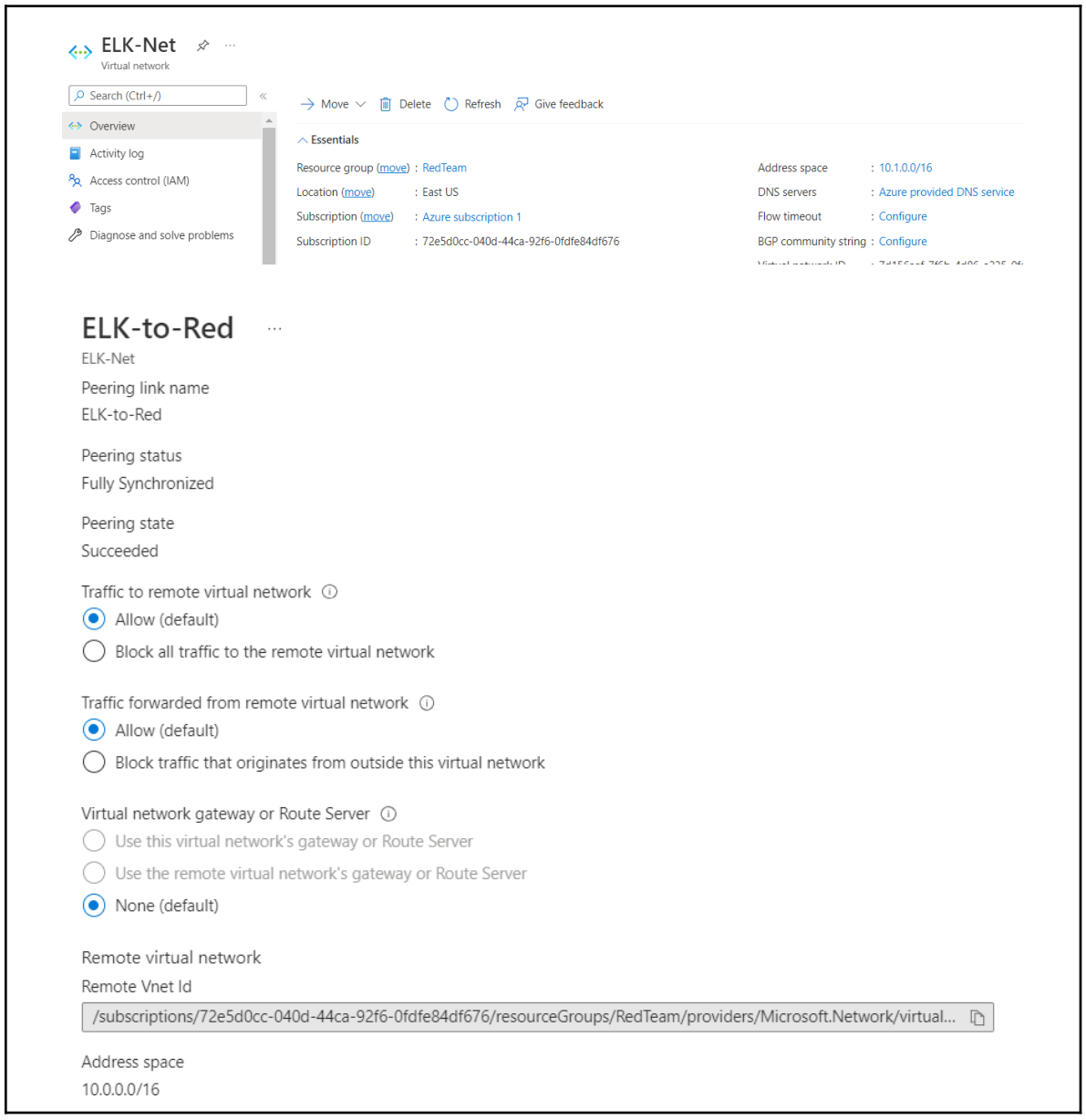
- cd /etc/ansible

-Nano ansible.cfg to specify the remote user.

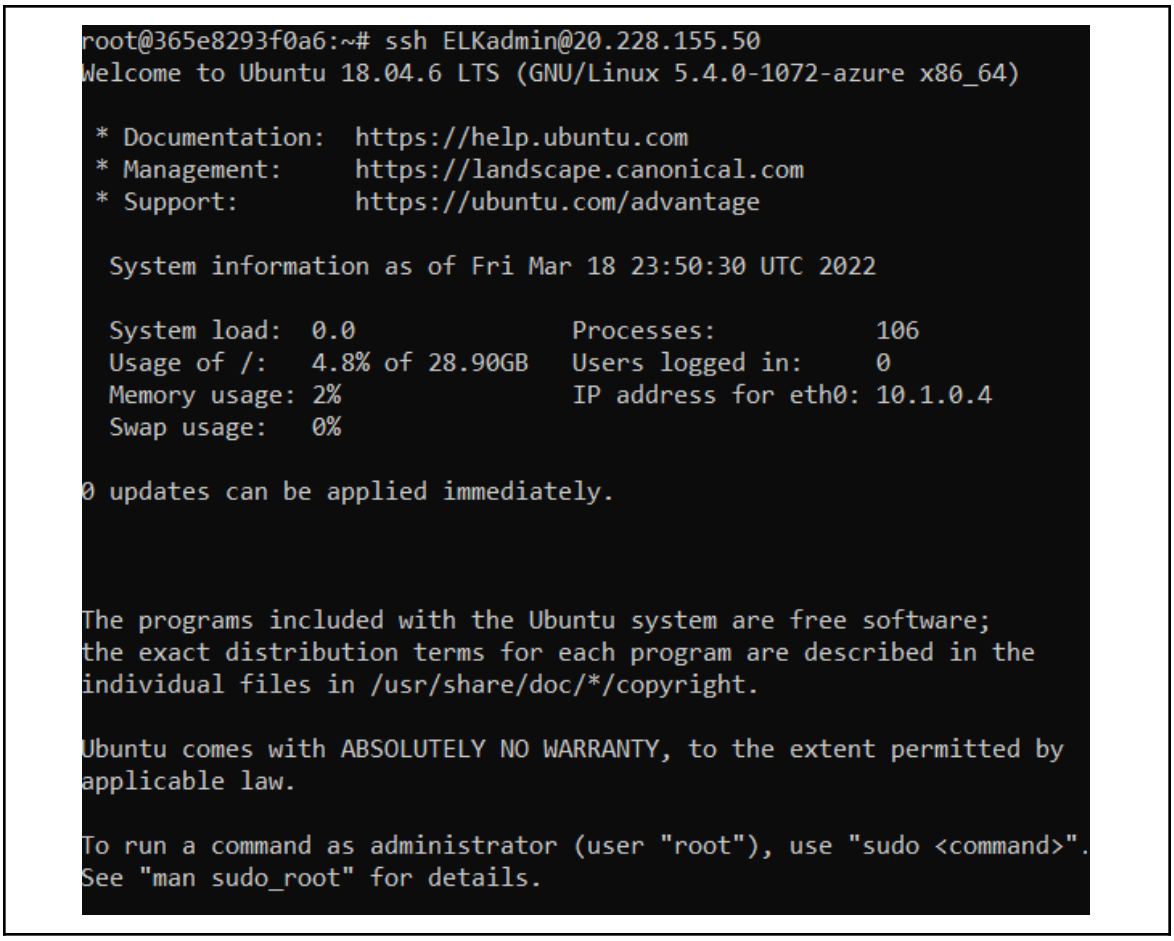
-ansible-playbook [name of playbook]

Steps:

1. Create a new vNet in a new region, within your resource group.

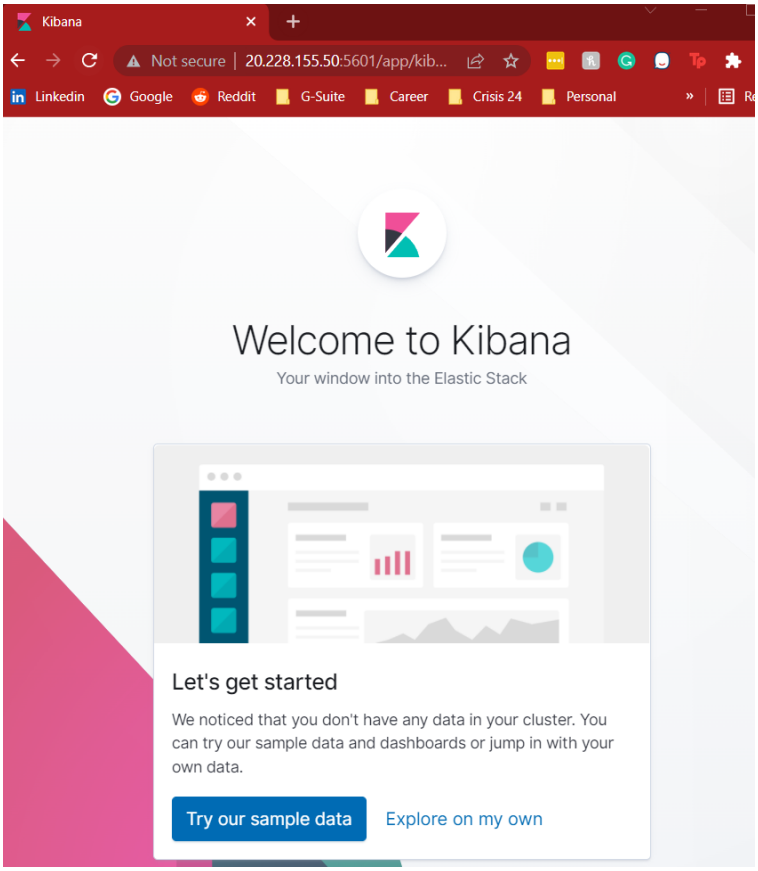


2. Create a new Ubuntu Virtual Machine.

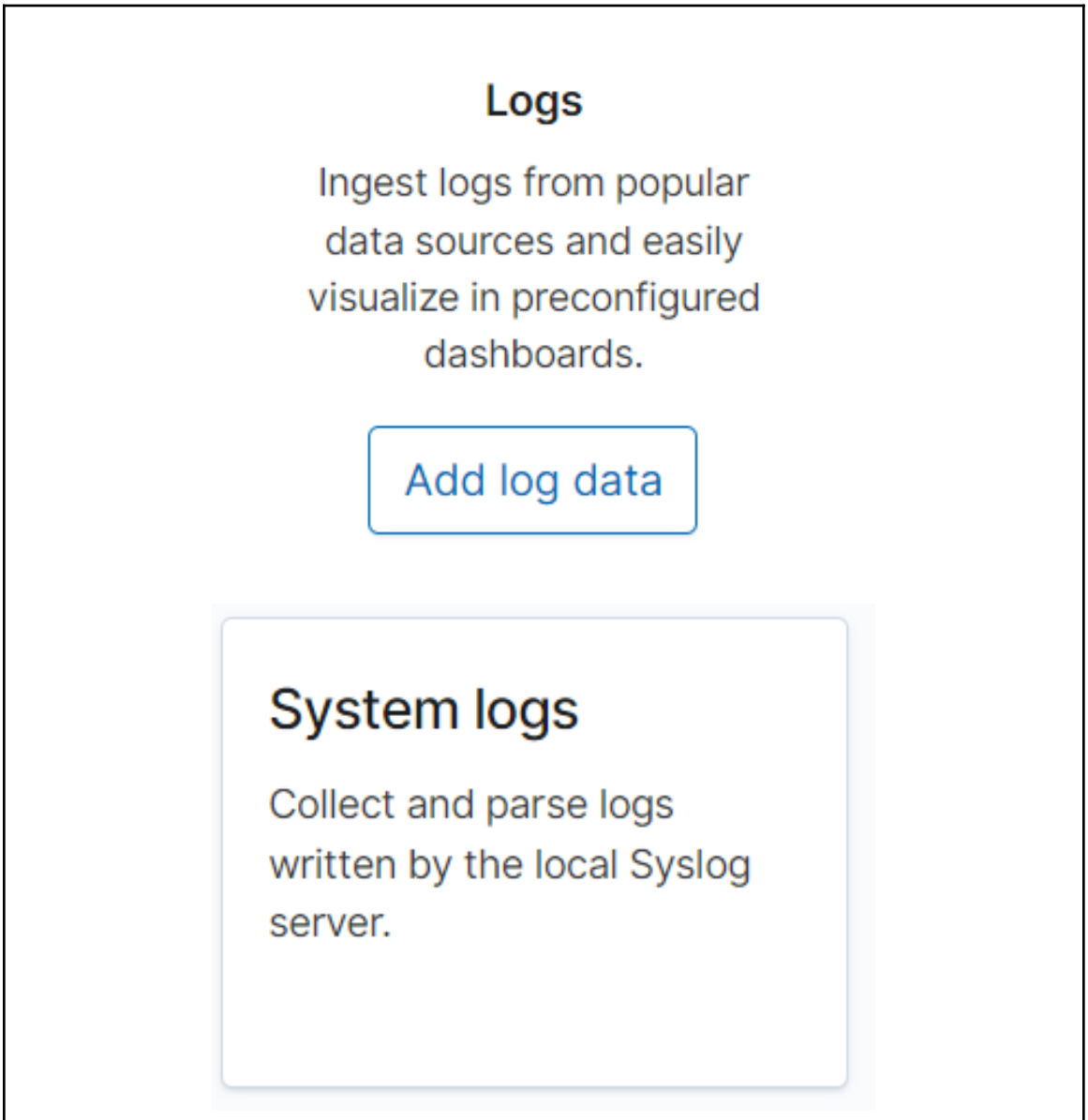


3. Launch and expose the container.

```
root@365e8293f0a6:/etc/ansible# ansible-playbook installelk.yml
[WARNING]: ansible.utils.display.initialize_locale has not been called, this may result in incorrectly calculated text
widths that can cause Display to print incorrect line lengths

PLAY [Configure Elk VM with Docker] ********************************************************************************
TASK [Gathering Facts] *********************************************************************************************ok
: [10.1.0.4]

TASK [Install docker.io] *******************************************************************************************ok
: [10.1.0.4]

TASK [Install python3-pip] *****************************************************************************************ok
: [10.1.0.4]

TASK [Install Docker module] ***************************************************************************************ok
: [10.1.0.4]

TASK [Increase virtual memory] *************************************************************************************ch
anged: [10.1.0.4]

TASK [Use more memory] *********************************************************************************************ok
: [10.1.0.4]

TASK [download and launch a docker elk container] ******************************************************************[D
EPRECATION WARNING]: The container_default_behavior option will change its default value from "compatibility" to
"no_defaults" in community.docker 2.0.0. To remove this warning, please specify an explicit value for it now. This
feature will be removed from community.docker in version 2.0.0. Deprecation warnings can be disabled by setting
deprecation_warnings=False in ansible.cfg.
changed: [10.1.0.4]

TASK [Enable service docker on boot] *******************************************************************************ok
: [10.1.0.4]

PLAY RECAP *********************************************************************************************************10
.1.0.4                     : ok=8    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

root@365e8293f0a6:/etc/ansible#
```



4. Install Filebeat on the Web VMs.



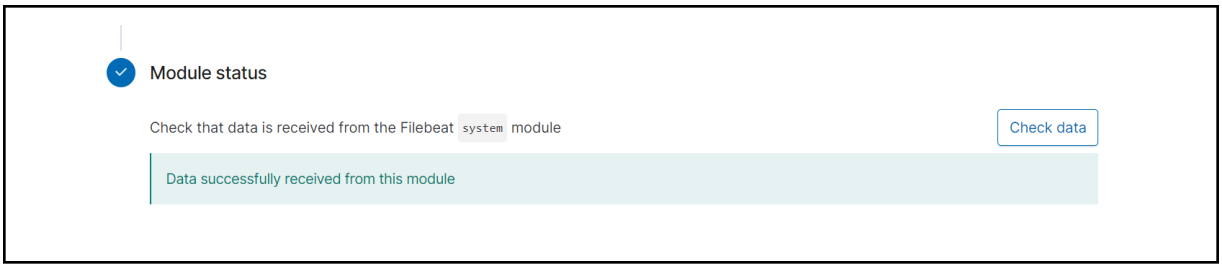

```
root@365e8293f0a6:~# curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-amd64.deb
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 23.9M  100 23.9M    0     0  76.1M      0 --:--:-- --:--:-- --:--:-- 76.1M
root@365e8293f0a6:~# ls
filebeat-7.6.1-amd64.deb
root@365e8293f0a6:~# sudo dpkg -i filebeat-7.6.1-amd64.deb
bash: sudo: command not found
root@365e8293f0a6:~# dpkg -i filebeat-7.6.1-amd64.deb
Selecting previously unselected package filebeat.
(Reading database ... 18241 files and directories currently installed.)
Preparing to unpack filebeat-7.6.1-amd64.deb ...
Unpacking filebeat (7.6.1) ...
Setting up filebeat (7.6.1) ...
```

5. Create the Filebeat installation play.

```
 GNU nano 4.8                                                    filebeat-playbook.yml
---
- name: installing and launching filebeat
  hosts: webservers
  become: yes
  tasks:

  - name: download filebeat deb
    command: curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-amd64.deb

  - name: install filebeat deb
    command: dpkg -i filebeat-7.6.1-amd64.deb

  - name: drop in filebeat.yml
    copy:
      src: /etc/ansible/filebeat-config.yml
      dest: /etc/filebeat/filebeat.yml

  - name: enable and configure system module
    command: filebeat modules enable system

  - name: setup filebeat
    command: filebeat setup

  - name: start filebeat service
    command: service filebeat start

  - name: enable service filebeat on boot
    systemd:
      name: filebeat
      enabled: yes
```

6. Verify the installation and playbook.

```
root@365e8293f0a6:/etc/ansible/roles# ansible-playbook filebeat-playbook.yml
[WARNING]: ansible.utils.display.initialize_locale has not been called, this may result in incorrectly calculated
text widths that can cause Display to print incorrect line lengths

PLAY [installing and launching filebeat] ***************************************************************

TASK [Gathering Facts] *********************************************************************************ok: [10.0.0.5]
ok: [10.0.0.6]
ok: [10.0.0.7]

TASK [download filebeat deb] ***************************************************************************changed: [10.0.0.6]
changed: [10.0.0.5]
changed: [10.0.0.7]

TASK [install filebeat deb] ****************************************************************************changed: [10.0.0.7]
changed: [10.0.0.6]
changed: [10.0.0.5]

TASK [drop in filebeat.yml] ****************************************************************************changed: [10.0.0.5]
changed: [10.0.0.7]
changed: [10.0.0.6]

TASK [enable and configure system module] **************************************************************changed: [10.0.0.5]
changed: [10.0.0.6]
changed: [10.0.0.7]

TASK [setup filebeat] **********************************************************************************changed: [10.0.0.5]
changed: [10.0.0.7]
changed: [10.0.0.6]

TASK [start filebeat service] **************************************************************************changed: [10.0.0.5]
changed: [10.0.0.7]
changed: [10.0.0.6]

TASK [enable service filebeat on boot] *****************************************************************changed: [10.0.0.5]
changed: [10.0.0.6]
changed: [10.0.0.7]

root@365e8293f0a6:/etc/ansible/roles#
ued=0    ignored=0
10.0.0.6                   : ok=8    changed=7    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.0.0.7                   : ok=8    changed=7    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

root@365e8293f0a6:/etc/ansible/roles#
```



7. Complete the same steps with Metricbeat.

```
  GNU nano 4.8                                                  metricbeat-playbook.yml
---
- name: Install metric beat
  hosts: webservers
  become: true
  tasks:
    # Use command module
  - name: Download metricbeat
    command: curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.6.1-amd64.deb

    # Use command module
  - name: install metricbeat
    command: dpkg -i metricbeat-7.6.1-amd64.deb

    # Use copy module
  - name: drop in metricbeat config
    copy:
      src: /etc/ansible/metricbeat-config.yml
      dest: /etc/metricbeat/metricbeat.yml

    # Use command module
  - name: enable and configure docker module for metric beat
    command: metricbeat modules enable docker

    # Use command module
  - name: setup metric beat
    command: metricbeat setup

    # Use command module
  - name: start metric beat
    command: service metricbeat start

    # Use systemd module
  - name: enable service metricbeat on boot
    systemd:
      name: metricbeat
      enabled: yes
```

```
root@365e8293f0a6:/etc/ansible/roles# ansible-playbook metricbeat-playbook.yml
[WARNING]: ansible.utils.display.initialize_locale has not been called, this may result in incorrectly calculated text
widths that can cause Display to print incorrect line lengths

PLAY [Install metric beat] ***************************************************************************************
TASK [Gathering Facts] *******************************************************************************************ok: [10.0.0.7]
ok: [10.0.0.5]
ok: [10.0.0.6]

TASK [Download metricbeat] ***************************************************************************************changed: [10.0.0.5]
changed: [10.0.0.7]
changed: [10.0.0.6]

TASK [install metricbeat] ****************************************************************************************changed: [10.0.0.7]
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [drop in metricbeat config] *********************************************************************************changed: [10.0.0.7]
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [enable and configure docker module for metric beat] ********************************************************changed: [10.0.0.5]
changed: [10.0.0.7]
changed: [10.0.0.6]

TASK [setup metric beat] *****************************************************************************************changed: [10.0.0.6]
changed: [10.0.0.5]
changed: [10.0.0.7]

TASK [start metric beat] *****************************************************************************************changed: [10.0.0.5]
changed: [10.0.0.7]
changed: [10.0.0.6]

TASK [enable service metricbeat on boot] *************************************************************************changed: [10.0.0.5]
changed: [10.0.0.7]
changed: [10.0.0.6]

PLAY RECAP *******************************************************************************************************10.0.0.5
 rescued=0    ignored=0
10.0.0.6                   : ok=8    changed=7    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.0.0.7                   : ok=8    changed=7    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

root@365e8293f0a6:/etc/ansible/roles#
```

Module status

Check that data is received from the Metricbeat `docker` module

Check data

Data successfully received from this module